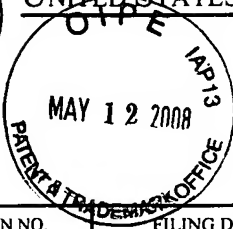




UNITED STATES PATENT AND TRADEMARK OFFICE

TFW



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/824,806	04/15/2004	Randolph Michael Forlenza	AUS920030938US1	6685

7590	04/29/2008
Darcell Walker Suite 250 9301 Southwest Freeway Houston, TX 77074	

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/824,806	Applicant(s) FORLENZA ET AL.	
	Examiner MATTHEW T. HENNING	Art Unit 2131	

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 April 2004.
 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 25-27 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) ☐ Claim(s) _____ is/are allowed.
 6) ☒ Claim(s) 25-27 is/are rejected.
 7) ☐ Claim(s) _____ is/are objected to.
 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
 10) ☒ The drawing(s) filed on 15 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>4/15/2004</u> . | 6) <input type="checkbox"/> Other: _____ |

1 This action is in response to the communication filed on 3/25/2008.

2 **DETAILED ACTION**

3 Claims 25-27 have been examined.

4 ***Title***

5 The title of the invention is acceptable.

6 ***Information Disclosure Statement***

7 The information disclosure statement(s) (IDS) submitted on 4/15/2004 are in compliance
8 with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information
9 disclosure statements.

10 ***Drawings***

11 The drawings filed on 4/15/2004 are acceptable for examination proceedings.

12 ***Claim Rejections - 35 USC § 102***

13 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis
14 for the rejections under this section made in this Office action:

15 *A person shall be entitled to a patent unless –*

16 *(e) the invention was described in (1) an application for patent, published under section*
17 *122(b), by another filed in the United States before the invention by the applicant for patent or*
18 *(2) a patent granted on an application for patent by another filed in the United States before the*
19 *invention by the applicant for patent, except that an international application filed under the*
20 *treaty defined in section 351(a) shall have the effects for purposes of this subsection of an*
21 *application filed in the United States only if the international application designated the United*
22 *States and was published under Article 21(2) of such treaty in the English language.*
23

24 Claim 25 is rejected under 35 U.S.C. 102(e) as being anticipated by Redlich et al. (US
25 Patent Number 7,322,047), hereinafter referred to as Redlich.

1 Regarding claim 25, Redlich disclosed a method for selective encryption within a
2 document comprising: detecting a document encryption request (Redlich Col. 53 Lines 10-33:
3 Step 612); activating a document encryption routine (Redlich Col. 53 Lines 10-33: Email
4 Security System Begins); accessing a proposed document for encryption and tagging one or
5 more sections of the proposed document as designated for encryption (Redlich Col. 53 Lines 10-
6 33: Step 612 Highlighting); encrypting the tagged sections with multiple encryption keys
7 (Redlich Col. 53 Lines 10-33: Step 618 and Col. 48 Lines 42-55: different cipher keys);
8 extracting the encrypted sections from the document (Redlich Col. 53 Lines 10-33: Step 616);
9 marking locations in the document where the extracted sections were located (Redlich Col. 51
10 Lines 21-27: Placeholders); storing extracted sections from the document in an appendix
11 attached to the document (Redlich Col. 53 Lines 38-40: secured data in encrypted form is
12 attached or appended to the original e-mail containing remainder data); receiving a request to
13 access an encrypted section of the document (Redlich Col. 54 Lines 28-34: addressee opens the
14 attachment); determining whether a received decryption key for the encrypted section of the
15 document for which the access request was made is proper for that encrypted section (Redlich
16 Col. 54 Lines 56-64, Col. 49 Lines 2-11, and Col. 39 Lines 26-45: detects and confirms the users
17 clearance level...and cleared data...is sent to the respective user); when the determination is that
18 the received decryption key is proper, retrieving and decrypting the section of the document for
19 which the access request was made (Redlich Col. 54 Lines 56-64, Col. 49 Lines 2-11, and Col.
20 39 Lines 26-45: detects and confirms the users clearance level...and cleared data...is sent to the
21 respective user); and displaying the decrypted section of the document (Redlich Col. 37 Lines
22 19-21).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Redlich. While Redlich disclosed determining whether there is a request to access another encrypted section of the document (Redlich Col. 54 Lines 56-64, Col. 49 Lines 2-11, and Col. 39 Lines 26-45: detects and confirms the users clearance level...and cleared data...is sent to the respective user); and when there is determination that there is a request to access another encrypted section of the document, repeating the steps of: determining whether a received decryption key for the encrypted section of the document for which the access request was made is proper for that encrypted section; when the determination is that the received decryption key is proper, retrieving and decrypting the section of the document for which the access request was made; and displaying the decrypted section of the document (Redlich Col. 54 Lines 56-64, Col. 49 Lines 2-11, and Col. 39 Lines 26-45: detects and confirms the users clearance level...and cleared data...is sent to the respective user), Redlich failed to specifically disclose the other request occurring after the first displaying. However, Redlich did disclose multiple users with varying security clearances accessing different portions of the document (Redlich Col. 39 Lines 26-45).

Conclusion

Claims 25-27 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent
2 Application Information Retrieval (PAIR) system. Status information for published applications
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
4 applications is available through Private PAIR only. For more information about the PAIR
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would
7 like assistance from a USPTO Customer Service Representative or access to the automated
8 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

9
10
11 /Matthew T Henning/
12 Examiner, Art Unit 2131
13 /Ayaz R. Sheikh/
14 Supervisory Patent Examiner, Art Unit 2131

Notice of References Cited	Application/Control No. 10/824,806	Applicant(s)/Patent Under Reexamination FORLENZA ET AL.	
	Examiner MATTHEW T. HENNING	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,322,047 B2	01-2008	Redlich et al.	726/27
*	B	US-6,598,161 B1	07-2003	Kluttz et al.	713/166
*	C	US-6,941,459 B1	09-2005	Hind et al.	713/167
*	D	US-7,103,915 B2	09-2006	Redlich et al.	726/27
*	E	US-2003/0110131 A1	06-2003	Alain et al.	705/51
*	F	US-7,178,033 B1	02-2007	Garcia, Denis Jacques Paul	713/184
*	G	US-6,868,495 B1	03-2005	Glover, John J.	713/190
*	H	US-5,933,498 A	08-1999	Schneck et al.	705/54
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	WO 02/01271 A1	01-2002	WO	Krasinski et al.	G02B 21/00
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01271 A1

(51) International Patent Classification⁷: G02B 21/00, (74) Agent: HOEKSTRA, Jelle; Internationaal Octrooibureau
21/16 B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

(21) International Application Number: PCT/EP01/07090 (81) Designated States (*national*): CN, JP, KR.

(22) International Filing Date: 22 June 2001 (22.06.2001) (84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

(25) Filing Language: English

(26) Publication Language: English

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

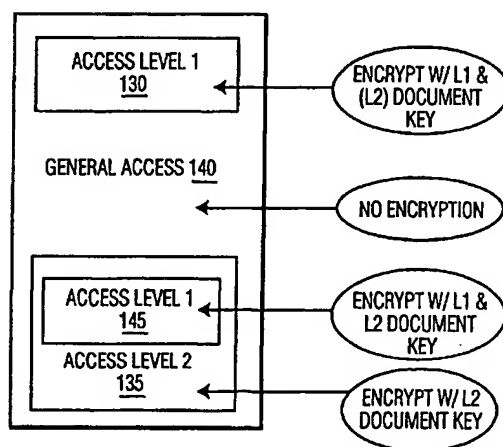
(30) Priority Data:
09/606,339 29 June 2000 (29.06.2000) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(72) Inventors: KRASINSKI, Raymond; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). ROSNER, Martin; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(54) Title: MULTIPLE ENCRYPTION OF A SINGLE DOCUMENT PROVIDING MULTIPLE LEVEL ACCESS PRIVILEGES



(57) Abstract: A method and system for selectively encrypting and decrypting different sections of a document provides different access levels in a technique employing different keys. The documents may be encrypted at a document section level ("section" here used according to its general meaning) and uses a different set of encryption keys for each section. A user A with an access level 1 may access only those section encoded with access level 1 plus unencoded sections. An application example of this technique is in hospitals. A patients records may each be segmented into separately-encrypted portions giving access to nurses for only suitable material while giving broader access to doctors. The nurse would be provided with his/her access level private key to gain access to those parts of the document for which nurses have rights. There could also be a level to which only the primary care physician or health care proxy has access.

WO 02/01271 A1

Multiple encryption of a single document providing multiple level access privileges

5

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The invention relates to document encryption and access restrictions on documents and more particularly to the encryption of each portion of a document such that access rights to respective portions may be obtained with corresponding keys.

BACKGROUND

Various kinds of document access protection are known. In one example, EP 0 848 314 A1 for DOCUMENT SECURITY SYSTEM AND METHOD only documents to which the user has rights are generated from a database. Varying security levels are provided. Another system described in US Patent No. 5,052,040 for MULTIPLE USER STORED DATA CRYPTOGRAPHIC LABELING SYSTEM AND METHOD permits different users to utilize the same files. The system exploits an extension of the file label which contains configuration capabilities and user rights and privileges. The separate user rights and privileges in this case relate to the entire document such as read only, read and write, deletion, etc. The document is encrypted. Another prior art system is described in US Patent No. 6,011,847 for CRYPTOGRAPHIC ACCESS AND LABELING SYSTEM. In this system, encryption and decryption of files uses a relational key generated by the system. A computer program also generates a series of labels that are encrypted and appended as a trailer to the encrypted message. The encrypted labels provide a history behind the particular encryption and they can be individually selected, separated, and decrypted from the total file.

An access control module provides access to an encryption portion of the document to users with passphrases by comparing a generated vector or key with a partially decrypted version of a second vector or key stored on a portable storage medium such as a floppy disk. In response, a main key can be generated to encrypt or decrypt the labels. The latter system is mainly concerned with adding descriptive labels to the end of an encrypted document and contains a key exchange method for passing the decryption key between a server and a client.

Other prior art systems and methods are known, but none contain a very convenient, robust, and straightforward method for encryption-protection of different parts of a document based on access privileges.

SUMMARY OF THE INVENTION

A method and system for selectively encrypting and decrypting different sections of a document provides different access levels in a technique employing different keys. The documents may be encrypted at a document section level ("section" here used according to its general meaning) and uses a different set of encryption keys for each section. A user A with an access level 1 may access only those sections encoded with access level 1 plus unencoded sections. An application example of this technique is in hospitals. A patients records may each be segmented into separately-encrypted portions giving access to nurses for only suitable material while giving broader access to doctors. Thus, this example illustrates access control to information contained inside a document based on pre-defined roles accepted within a specific environment. The nurse would be provided with an access level key based on the access control rules defined by the hospital. Such key would allow the nurse to gain access to those parts of the document for which nurses have rights. There could also be a level to which only the primary care physician or health care proxy has access.

A method for distributing keys is also provided. This method utilizes a key box which is created for holding keys used to encode the sections of the document. The key box contains a slot for each level of access. The set of keys that a user at a given level requires is placed in a corresponding slot. Each slot is encoded using the access level public key giving the user access to the keys in the appropriate slot when decrypted using the user's private key.

An additional feature provides an outer layer of encryption using a public key for a requesting organization. Once the requesting organization opens the document using its private key, anyone in the receiving organization can apply their access level private key(s) to the key box, which in turn applies the keys in the corresponding slot to the document. This allows each user to view/modify the parts of the document to which they have access rights.

The invention will be described in connection with certain preferred embodiments, with reference to the following illustrative figures so that it may be more fully understood. The description of this invention uses the definition of public key to correspond to the public portion of the public/private key pair that is used in the art to realize asymmetric algorithms. The description of this invention uses the definition of private key to correspond to the private portion of the public/private key pair that is used in the art to realize asymmetric algorithms. The description of this invention uses the definition of symmetric key to refer to the a single key that is used in the art to realize symmetric algorithms.

With reference to the figures, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice.

10 BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is an illustration of a computer environment in which the invention may be used.

Fig. 2A is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to first embodiment of the invention in which public keys are used for encryption.

Fig. 2B is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to second embodiment of the invention in which public keys are used for encryption.

Fig. 3 is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to third embodiment of the invention in which document-specific keys are used.

Fig. 4 is an illustration of a key box document used with the embodiment of Fig. 3.

Fig. 5 is an illustration of a process for encrypting a document according to an embodiment compatible with any of the foregoing embodiments.

Fig. 6 is an illustration of a process for encrypting a document according to an embodiment compatible with any of the foregoing embodiments.

Fig. 7 is an alternative way of packaging the key box in a transmission by including it within a single document.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to Fig. 1, the invention may be used in the environment of electronic document transfer. An example of such an environment is a sending computer 110 and a

receiving computer 120 connected by a network 100 or simply by physical transfer of a non-volatile data store 90 such as a floppy disk.

Referring to Fig. 2A, a document 95 contains various sections 130, 135, 140, and 145. Each section is divided according to how the information contained in the section is desired to be made available to a particular person (organization or other entity) or class of persons. The document 95 is intended to be transferred by the sender 110 to the receiver 120, the receiver including each of the persons or classes of persons. The sections labeled 130 and 145 are encrypted with a public key L1 corresponding to the first user or class of users. The section labeled 135 is encrypted with a second public key L2 corresponding to the second user or class of users. By virtue of being embedded in the section 135, section 145 is also encrypted with the L2 public key.

Referring to Fig. 2B, the various sections may be encrypted with only one key or all keys from the access level to which they correspond down to the lowest level of access. Thus, in this example, document section 145 is encrypted with both the L1 and L2 keys, but so is document section 130. Alternatively, each section may be encrypted with only a single key, so that a level 1 section appearing in a level 2 section is simply treated as a completely separate section with the level 2 section being broken into separate subsections for L2 encryption. The encryption methods described above permit multilevel access to a document based on the public keys of the intended audience. It is possible to limit access based on the user as well as the particular document as shown in the next embodiment.

Referring now to Figs. 3 and 4, the document sections are encrypted with respective document keys, a respective one for each access level defined within the scope of the document. The document keys may be symmetric keys. The latter are not shared outside of the context of use of the document and the user need never directly know what the symmetric keys are. These document keys are then made available to the recipients by encrypting them into a separate document (which could be part of the original document as in a file header as illustrated in Fig. 7) called a key box. The key box has a slot corresponding to each access level defined within the scope of the organization that is requesting such document. A first slot 1 210 contains document keys for access levels 1 and 2 giving the user access to both levels. A second slot 1 215 contains document keys for access level 2. Each slot is encrypted using the public key of the organization that corresponds to the access level of the slot. The entire key box file and the document may be encrypted using the public key of the user to ensure confidentiality of the transmission of the document and the key box.

Additionally, the key box and the document may be signed by the sender 110 to ensure integrity of the transmission and authenticity of the document.

The preceding embodiment contemplates an agreement between the sender of the document who prepares the encryption and the organization receiving the document.

- 5 This agreement would map access levels used in encrypting the document to the access levels in place at the receiver. For a given document, a given organization level may map to a single document access level. Alternatively, a given organization level may map to multiple document access level.

- 10 Preferably, to assure data integrity and non-repudiation, the document source may sign the document hash with a private key. The requestor receiving the document together with the signature can then vouch for the validity of the source. Other mechanisms for authenticating the document's contents may also be used.

- 15 When a person with access level N opens the document, he/she presents his/her organization access level private key, which corresponds to the asymmetric key pair, to a decryption process that uses the key to access the appropriate slot in the key box. The symmetric keys may be used by the process to access the appropriate levels of the document transparently to the user. The user never "handles" the symmetric document keys and simply accesses the portions of the document the user has permission to access.

- 20 Referring now to Fig. 5, the detailed steps for creating, sending, receiving, and using a document begin with the receipt of a request S10 for the document and the appropriate information such as the public keys of the users, a map of users to access levels, etc. Next, a key is created for each access level required S20. The document is then encrypted starting with the highest (most privileged) access level and going down S30. This may result in the layered encryption of either of Figs. 2A and 2B or the alternative process
25 where each level is only encrypted once. The keys are formed into a key box document and each set separately encrypted using the public keys of the access levels S45. Then the document and key box are bundled and optionally encrypted using the public key of the receiver S55.

- 30 When the receiver receives the file containing the encrypted document and the key box, the package is unbundled and optionally decrypted S60. The document and key box are then made available to the users S70. When a user accesses the document, the user provides his/her organization access level private key to a decryption process on a receiving computer (e.g. 120) which uses the key to decrypt the appropriate slot of the key box S75. The process then applies the symmetric keys, obtained from the decrypted slot in the key

box, S80 to the document to allow the user to access the document S85. The user never directly accesses the symmetric access level keys or even concerns him/herself with how many keys are involved.

Referring to Fig. 6, in an alternative embodiment, the public keys of the
5 receivers are not used to encrypt the document. Rather step S45 is skipped and the key box is simply encrypted using the organization's public key. At the receiving organization, an additional step S90 between S65 and S70 is added wherein the slots of the key box are mapped to the access levels present in the organization and encrypted with the appropriate public keys of the users or group of users.

10 It will be evident to those skilled in the art that the invention is not limited to the details of the foregoing illustrative embodiments, and that the present invention may be embodied in other specific forms without departing from the spirit or essential attributes thereof. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended
15 claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

CLAIMS:

1. A method of securely transmitting a first document, comprising the steps of:
 - generating first and second level document keys;
 - encrypting a first section (130) of said first document with said first level document key and encrypting said first and a second section (135) of said first document with said second level document key;
 - 5 - forming a second document (220) or a portion (520) of said document, said second document or said portion containing said first and second level document keys;
 - transmitting said first document or said first and second documents as appropriate to the choice in said step of forming.
- 10 2. A method as in claim 1, wherein said first and second level document keys are symmetric keys.
3. A method as in claim 1, further comprising receiving at least two public keys
15 from a recipient, said step of forming including encrypting said second document such that a corresponding set of said first and second level document keys is made available by decryption using a first of said at least two public keys and such that a corresponding other set of said first and second level document keys is made available by decryption using said second of said at least two public keys.
- 20 4. A method as in claim 3, wherein said step of encrypting including encrypting a first of said at least two public keys in a first portion of said second document or first document portion and encrypting a first and second of said at least two public keys in a second portion of second document or first document portion.
- 25 5. A method as in claim 3, wherein said first and second level document keys are symmetric keys.

6. A method as in claim 1, wherein said step of transmitting includes encrypting said first document or said first and second documents as appropriate to the choice in said step of forming.

5 7. A method of encrypting a document, comprising the steps of:
- encrypting a first portion of a document using a first key;
- encrypting a second portion of said document using a second key;
- encrypting a result of said first and second steps of encrypting using a third key, being a public key of a recipient.

10

8. A method of encrypting a document as in claim 7, wherein said first key is a first public key of said recipient and said second key is a second public key of said recipient.

9. A method of encrypting a document as in claim 7, wherein said first key is a
15 first symmetric key and said second key is a second symmetric key, and the method includes the step of encrypting said first symmetric key with a public key.

10. A method as in claim 9, wherein said second portion includes a part of said first portion, said part having been encrypted with said first symmetric key.

20

11. A method of encrypting a document as in claim 9, comprising the step of encrypting said second symmetric key with a second public key.

12. A method of securely providing access to first and second readers of a
25 document, comprising the steps of:

- transmitting to a sender of a document, public keys corresponding to readers of said document, said public keys being used to encrypt said document;
- receiving encrypted data from said sender;

decrypted a portion of said encrypted data using a private key corresponding to one of said
30 public keys;

- a result of said first step decrypting being the accessing of a portion of said data corresponding to said one of said public keys;
- decrypting a portion of said encrypted data using a private key corresponding to another of said public keys;

- result of said second step decrypting being the accessing of a portion of said data corresponding to said other of said public keys.

13. A method as in claim 12, wherein said first and second steps of decrypting
5 each include decrypting a portion of said data to unlock a respective set of encryption keys.

14. A method as in claim 12, wherein said first and second steps of decrypting
further include using said respective set of encryption keys to unlock at least a portion of said
encrypted data to provide access to only a portion of said document.

10

15. A method as in claim 12, wherein said first and second steps of decrypting
further include using said respective set of encryption keys to unlock at least a portion of said
encrypted data to provide access to said document.

15 16. A data file (95+220), comprising:
an encryption protected document (95, 595) containing a key portion (520) and an encrypted
document portion (585);

- said key portion being at least partly decryptable with a first public key to
provide access to a first symmetric key;
20 - said key portion being at least partly decryptable with a second public key to
provide access to a second symmetric key;
- a first portion (210) of said encrypted document portion being decryptable
with said first symmetric key and a second portion (215) of said encrypted document portion
being decryptable with said second symmetric key.

25

17. A data file containing:
- an encrypted document (95) and at least two encryption keys;
- said encryption keys being encrypted such as to be accessible using at least
two public keys and such that a first portion (130) of said encrypted document is accessible
30 by decrypting with a first subset of said encryption keys, said first subset being decryptable
using a first of said at least two public keys, and such that a second portion of said encrypted
document is accessible by decrypting with a second subset of said encryption keys, said
second subset being decryptable using a second of said at least two public keys.

18. A data set stored on a data storage medium, comprising:
- a document encrypted in portions using respective keys to encrypt said portions;
 - a first portion of said document being encrypted with a first of said respective keys;
 - a second portion of said document being encrypted with a second of said respective key;
 - said first and second respective keys being encrypted in a file such as to permit decryption of said first key by a first private key and to permit decryption of said second key by a second private key.
19. A data set stored on a data storage medium, comprising:
- document encrypted in portions using respective keys to encrypt said portions;
 - a first portion of said document being encrypted with first and second of said respective keys;
 - a second portion of said document being encrypted with said first respective key;
 - said first and second respective keys being encrypted in a file such as to permit decryption of said first and second keys by a first private key and to permit decryption of said first key by a second private key.
20. A document decrypting program stored on a data storage medium, comprising:
- code defining a process capable of selectively decrypting a portion of a data set using a respective key, said portion yielding a respective set of further keys upon decryption;
 - code defining a further process capable of retrieving from said data set portions of a document corresponding to said respective set of further keys to provide access to only portions of said document corresponding to respective key.
21. A stored program as in claim 20, wherein said respective key is a public key.
22. A stored program as in claim 20, wherein each of said set of further keys is unique to said document.

23. A stored program as in claim 20, wherein each of said set of further keys is a symmetric key.

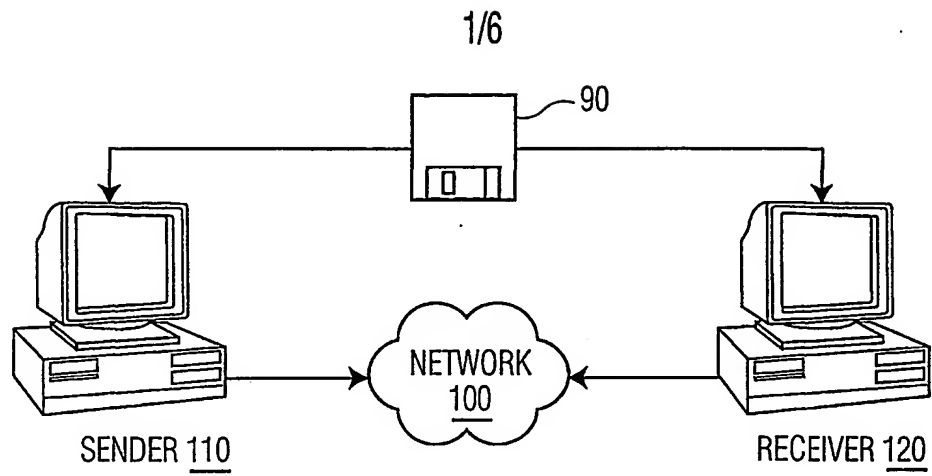


FIG. 1

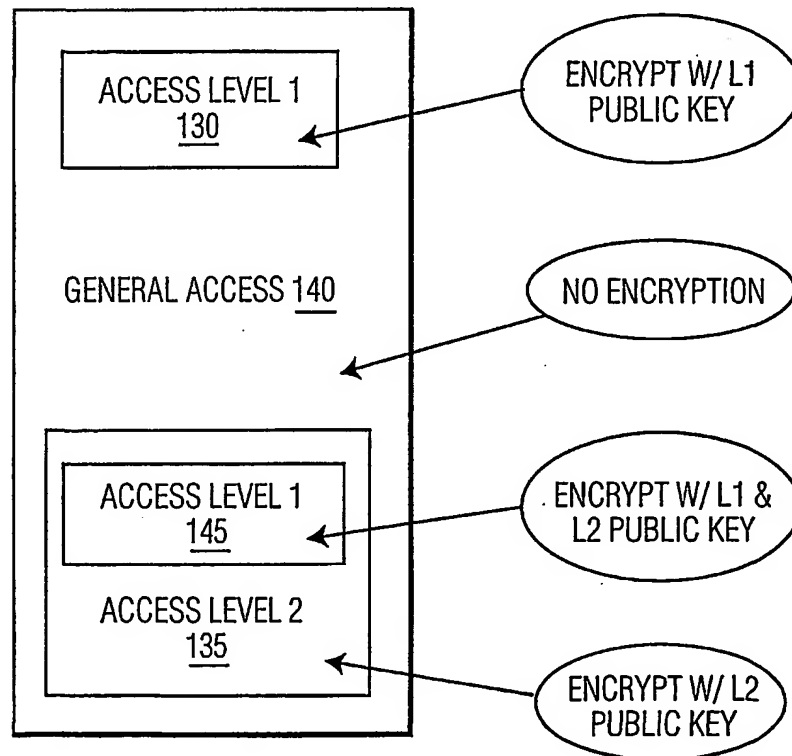


FIG. 2A

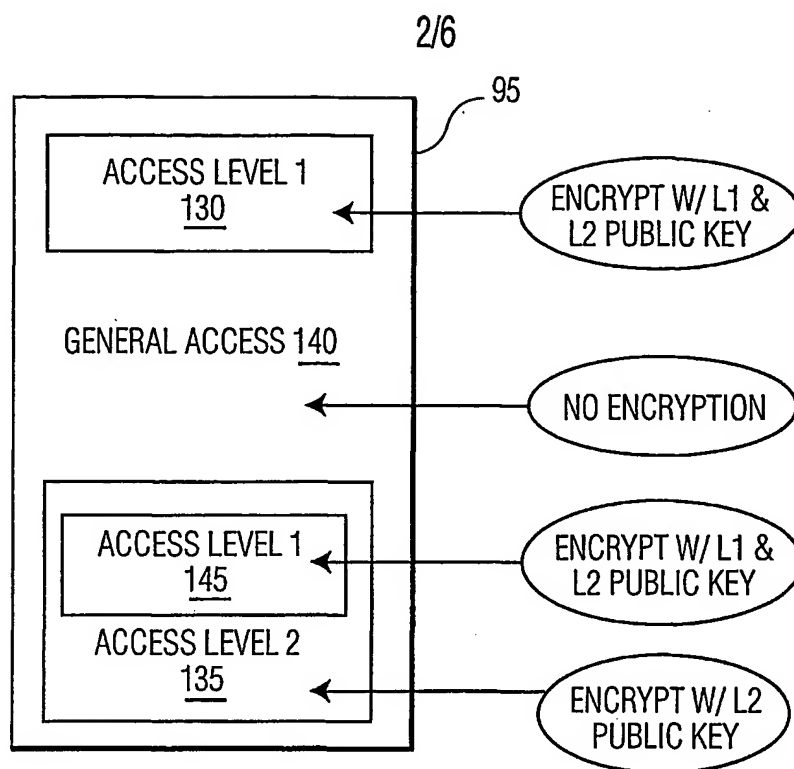


FIG. 2B

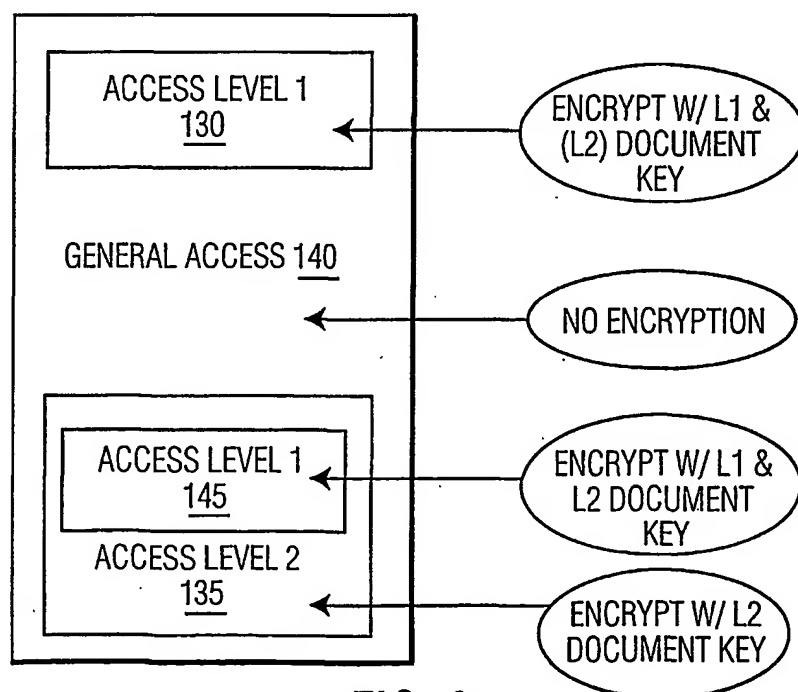


FIG. 3

3/6

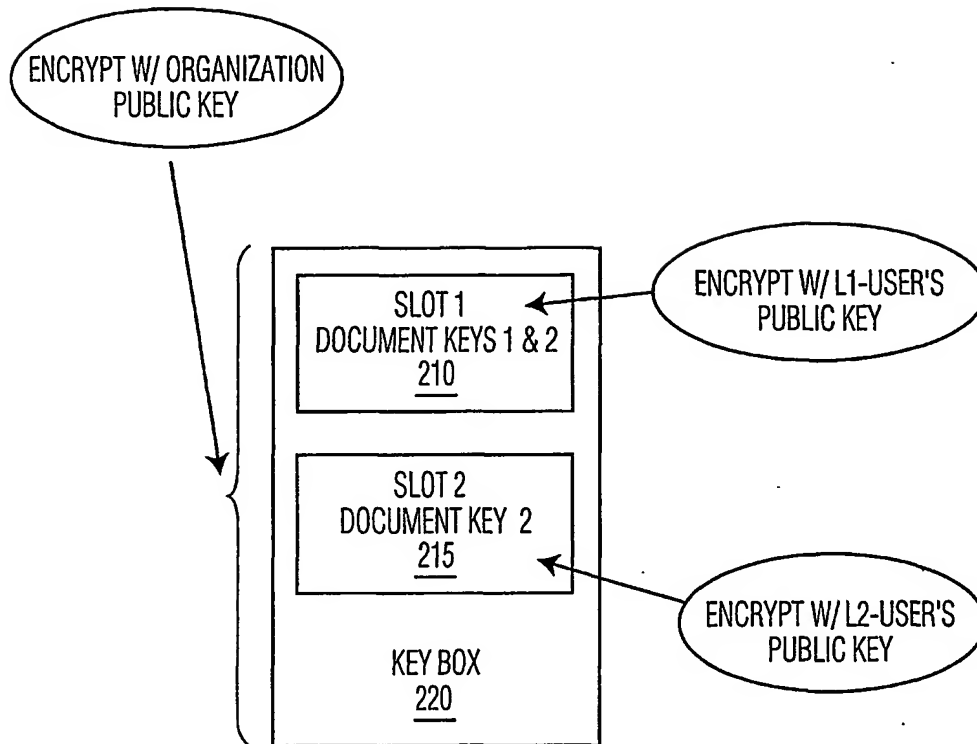


FIG. 4

4/6

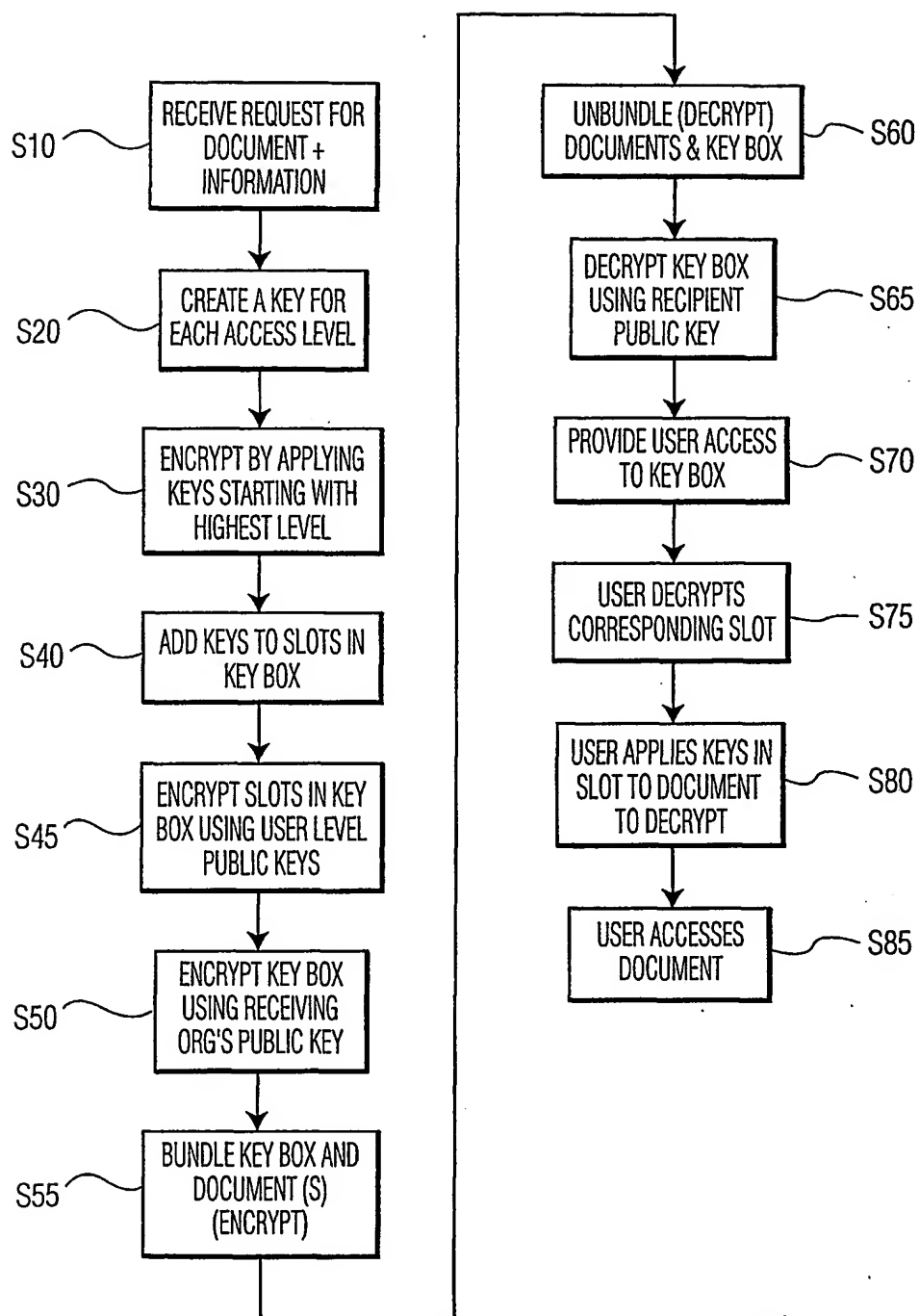


FIG. 5

5/6

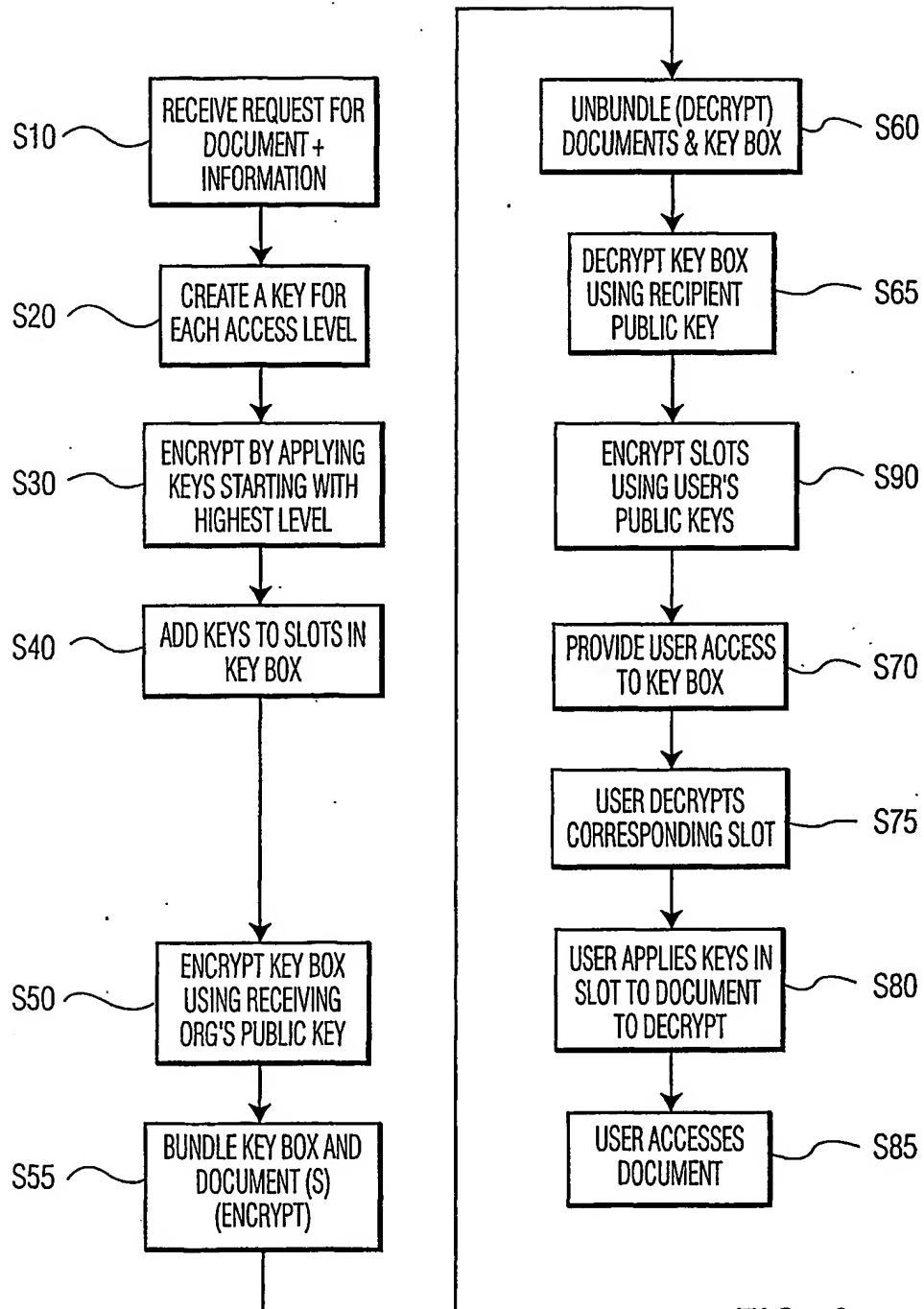


FIG. 6

6/6

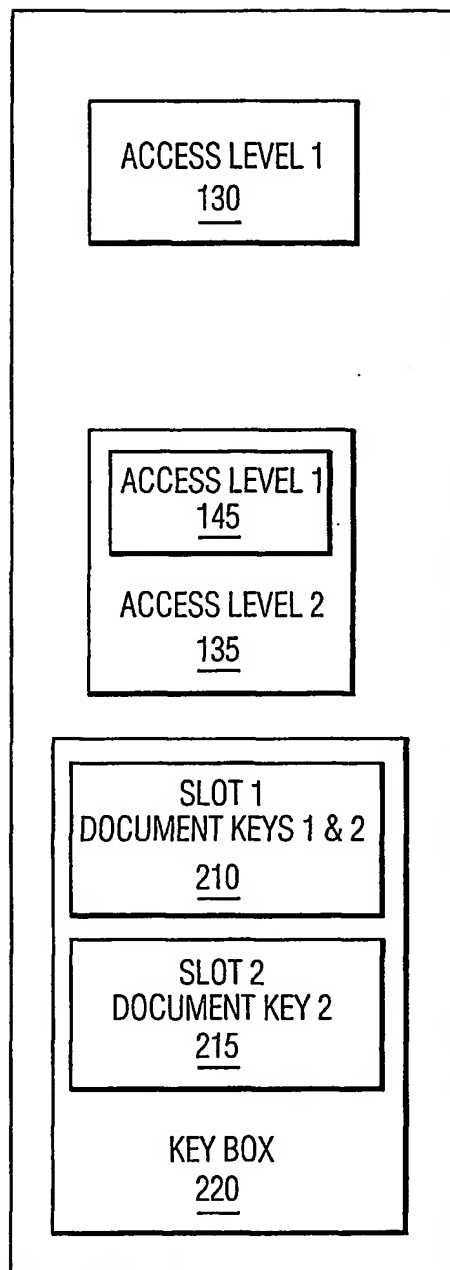


FIG. 7

EL978318025 US

PATENT
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: : Group Art Unit: unknown
Randolph Forlenza, et al. : Intellectual Property
Serial No: : Law Department
Filed: Herewith : International Business
: Machines Corporation
Title: Method for Selective Encryption : 11400 Burnet Road
Within Documents : Austin, Texas 78758

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

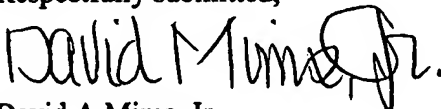
Applicants submit herewith patents, publications or other information of which they are aware, which they believe may be material to the patentability of this application and in respect of which there may be a duty to disclose in accordance with 37 CFR 1.56.

While this Information Disclosure Statement may be "material" pursuant to 37 CFR 1.56, it is not intended to constitute an admission that any patent, publication or other information referred to herein is "prior art" for this invention unless specifically designated as such.

In accordance with 37 CFR 1.97(g) the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR 1.56 (a) exists.

The attached form, PTO-1449, provides a listing of patents, publications, or other information as required by 37 CFR 1.98 (a)(1).

Respectfully submitted,



David A Mims, Jr.
Attorney
Registration No. 32,708
Telephone No. 512-823-0950

In Place of FORM PTO-1449 (Modified)

Serial No. 10/824,806

LIST OF PATENTS AND PUBLICATIONS FOR
APPLICANT'S INFORMATION DISCLOSURE
STATEMENT

Applicant: IBM Corporation

Filing Date:

Group:

Atty. Docket No. AUS920030938US1

Reference Designation

U. S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate
AA	5,673,316	09-30-97	Auerbach et al.	380	4	03-29-96
AB	6,339,825	01-15-02	Pensak et al.	715	158	07-18-01
AC	6,345,256	02-05-02	Milsted et al.	705	1	12-01-98
AD	6,449,721	09-10-02	Pensak et al.	713	171	11-01-01
AE						

FOREIGN PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation Yes No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner
Initial

AR
AS
AT
AU

Examiner: /Matthew Henning/

Date Considered: 04/22/2008

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Organization 102100 Bldg/Room
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
If Undeliverable Return in Ten Days

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300

AN EQUAL OPPORTUNITY EMPLOYER

WALKER 301* 770742005 1207 32 05/02/08
FORWARD TIME EXP RTN TO SEND
CARCEL WALKER ATTORNEY
3107 CARVEL LN
HOUSTON TX 77036-6317

RETURN TO SENDER
NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

RECEIVED
MAY 12 2008
USPTO MAIL CENTER

